U.S. Department of Homeland Security
Transportation Security Administration
6595 Springfield Center Drive
Springfield, Virginia 20598

MEMORANDUM

To: Covered Railroad Owner/Operators

Date: October 23, 2023

Subject: Renewal with revisions to the Security Directive 1580/82-2022-01 series: *Rail Cybersecurity Mitigation Actions and Testing*

Attached to this memorandum is Security Directive 1580/82-2022-01A, *Rail Cybersecurity Mitigation Actions and Testing.* This security directive is a continuation of the Security Directive 1580/82-2022-01 series and takes effect on October 24, 2023, extending the requirements for one year.

This security directive applies to each freight railroad carrier identified in 49 CFR 1580.101, and TSA-designated freight and passenger railroads. If TSA identifies additional railroad Owner/Operators who were not already subject to the Security Directive 1580/82-2022-01 series, TSA will notify these Owner/Operator(s) and provide specific compliance deadlines for the requirements in this security directive.

The substantive revisions in this security directive maintain TSA's performance-based cybersecurity requirements, which were first issued in October 2022. The security directive changes are summarized in the table below.

Section II.A.2.
This is a new section clarifying that if an Owner/Operator has delegated or shared responsibility to a *Managed Security Service Provider,*[1] wholly or in part, for security measures in the Owner/Operators CIP, the Owner/Operator retains sole responsibility under this security directive for ensuring compliance with the TSA-approved Cybersecurity Implementation Plan and the Security Directive (SD).

[1] TSA defines *Managed Security Service Providers*, for the purposes of this security directive, as a person who is not a direct employee of the owner/operator, but who provides one or more services or capabilities that the owner/operator is using to perform measures required by the security directive. Managed Security Service Providers are not Authorized Representatives.

U.S. Department of Homeland Security
Transportation Security Administration
6595 Springfield Center Drive
Springfield, Virginia 20598

Section II.A.3.
This is a new section clarifying that an *Authorized Representative*[2] is empowered by the Owner/Operator to coordinate and conduct activities required by this security directive. *Authorized Representatives* are liable for non-compliance separate or in addition to the Owner/Operator.
Section II.A.4. (Scope)
This section includes new language to inform Owner/Operators that TSA will notify them if the agency disagrees with the Owner/Operator's determination and may require the Owner/Operator to provide additional information regarding the methodologies or rationale used to identify Critical Cyber Systems. If applicable, the Owner/Operators needs to notify TSA within 60 days of the change in operations to determine the schedule for complying with the requirements of this SD.
Section II.B.3.
This is a new section clarifying that if an Owner/Operator needs to amend its TSA-approved Cybersecurity Implementation Plan (CIP) based on revisions to this SD, it must follow the procedures in Section VI.
Section III.A.
This section includes new language informing Owner/Operators that, following consultation, TSA may notify an Owner/Operator that it must include additional Critical Cyber Systems identified by TSA that the Owner/Operator has not previously identified in its CIP.
Section III.F.
This section replaces "Cybersecurity Assessment Program" with "Cybersecurity Assessment Plan" (CAP) to more accurately reflect the changes made in this SD.
This section includes a new requirement for a CAP schedule for assessing and auditing specific cybersecurity measures and/or actions. The schedule must ensure that at least one third of the policies, procedures, measures, and capabilities in the TSA-approved CIP are assessed each year so that 100 percent will be assessed every three years.
This section includes a new requirement for an annual CAP Report that must be submitted to TSA for review. The report must include the results of assessments conducted in accordance with the previous annual CAP and indicate which assessment method(s) were used to determine if the policies, procedures, and capabilities described by the Owner/Operator in its CIP are effective.
This section includes a new requirement that Owner/Operators must review and update their CAP on an annual basis. Owner/Operators will continue to submit an annual CAP not only for TSA review, but also for TSA approval. Subsequent annual CAPs will also require TSA approval.
This section includes a new requirement that Owner/Operators must submit their CAP Report on an annual basis, and the schedule for determining the due date.

[2] TSA defines *Authorized Representative*, for the purposes of this security directive, as a person who is not a direct employee of the owner/operator, but is authorized to act on the owner/operator's behalf to perform measures required by the security directive. The term authorized representative includes agents, contractors, and subcontractors. This term does not include Managed Security Service Providers.

U.S. Department of Homeland Security
Transportation Security Administration
6595 Springfield Center Drive
Springfield, Virginia 20598

Section IV.A.
This section includes revised language requiring that previously developed plans, assessments, tests, and evaluations used to meet the requirements of this security directive and previously listed in an index must now be explicitly incorporated by reference in the CIP and be made available to TSA upon request.
Section V.C.
This section includes a new requirement that Owner/Operators must submit documents in a manner prescribed by TSA. The language is being provided to provide flexibility for future capabilities.
Section VII.
This section includes new definitions for "Authorized Representative" and "Managed Security Service Providers"

Consistent with TSA's previous determination, this SD should not be marked as Sensitive Security Information (SSI). While SDs generally are categorically deemed SSI under TSA's regulations (49 CFR part 1520), TSA previously determined that the contents of this SD would not be detrimental to transportation security if publicly disclosed. No revisions to the previously approved Information Collection Request approved by the Office of Management and Budget are necessary to accommodate any information collected under the revision.

The security directive requires that railroad Owner/Operators provide written confirmation of receipt of this security directive via email to SurfOpsRail-SD@tsa.dhs.gov. All queries concerning the attached security directive should be submitted to TSA at TSA-Surface@tsa.dhs.gov.

STACEY D FITZMAURICE
Digitally signed by STACEY D FITZMAURICE
Date: 2023.10.20 15:47:20 -04'00'

Stacey Fitzmaurice
Executive Assistant Administrator
Operations Support

Attachment: Security Directive 1580/82-2022-01A

U.S. Department of Homeland Security
Transportation Security Administration
6595 Springfield Center Drive
Springfield, Virginia 20598

NUMBER	Security Directive 1580/82-2022-01**A**
SUBJECT	Rail Cybersecurity Mitigation Actions and Testing
EFFECTIVE DATE	**October 24, 2023**
EXPIRATION DATE	**October 24, 2024**
SUPERSEDES	**Security Directive 1580/82-2022-01**
APPLICABILITY	Each freight railroad carrier identified in 49 CFR 1580.101 and other TSA-designated freight and passenger railroads
AUTHORITY	49 U.S.C. 114(d), (f), (*l*) and (m)
LOCATION	All locations within the United States

I. PURPOSE AND GENERAL INFORMATION

The Transportation Security Administration (TSA) is issuing this Security Directive due to the ongoing cybersecurity threat to surface transportation systems and associated infrastructure to mitigate the significant harm to the national and economic security of the United States that could result from the "degradation, destruction, or malfunction of systems that control this infrastructure.[1]

This Security Directive **continues to require the same performance-based cybersecurity measures first issued by TSA in October 2022**.[2] The required actions continue to be necessary to protect the national security, economy, and public health and safety of the United States and its citizens from the impact of malicious cyber-intrusions affecting the nation's railroads.[3] Even minor disruptions in critical rail systems may result in temporary product shortages that can cause significant harm to national security. Prolonged disruptions in the flow of commodities could lead to widespread supply chain disruptions, with ripple

[1] *See National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems* (July 29, 2021).
[2] As noted in the Office of Management and Budget's Unified Agenda, TSA intends to more permanently codify these requirements through notice-and-comment rulemaking.
[3] This Security Directive is issued under the authority of 49 U.S.C. 114(*l*)(2)(A), which states: "Notwithstanding any other provision of law or executive order (including an executive order requiring a cost-benefit analysis), if the Administrator determines that a regulation or security directive must be issued immediately in order to protect transportation security, the Administrator shall issue the regulation or security directive without providing notice or an opportunity for comment and without prior approval of the Secretary."

effects across the economy. Disruptions and delays may affect industries that depend on the commodities transported by the nation's railroads.

The goal of this Security Directive is to reduce the risk that cybersecurity threats pose to critical railroad operations and facilities through implementation of layered cybersecurity measures that provide defense-in-depth. Recent and evolving intelligence emphasizes the growing sophistication of nefarious persons, organizations, and governments, highlights vulnerabilities, and intensifies the urgency of implementing the requirements of this Security Directive.[4]

In general, this Security Directive is applicable to the same railroads subject to the Security Directive 1580-21-01 series, "Enhancing Rail Cybersecurity,"[5] and additional TSA-designated freight and passenger railroads notified by TSA based on a risk determination. **All revisions to this Security Directive series from the previous version, SD 1580/82-2022-01, are highlighted in bold.**

To protect against the ongoing threat to the United States' national and economic security, this Security Directive mandates that these railroad Owner/Operators implement the following cybersecurity measures to prevent disruptions to their infrastructure and/or operations. Specifically, Owner/Operators must:

1. Establish and implement a TSA-approved Cybersecurity Implementation Plan that describes the specific measures employed and the schedule for achieving the following outcomes, as more fully described in Section III.A through III.E.:

    a. Implement network segmentation policies and controls to ensure that the Operational Technology system can continue to safely operate in the event that an Information Technology system has been compromised;

    b. Implement access control measures to secure and prevent unauthorized access to Critical Cyber Systems;

    c. Implement continuous monitoring and detection policies and procedures to detect cybersecurity threats and correct anomalies that affect Critical Cyber

[4] *See* Joint Cybersecurity Advisory (AA22-110A), Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure (dated April 20, 2022), available at https://www.cisa.gov/uscert/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf. **A**dditional information regarding current threats **is** posted at https://www.cisa.gov/shields-up. ***See also* Office of the Director of National Intelligence (ODNI), *Annual Threat Assessment of The U.S. Intelligence Community* (dated February 6, 2023), available at 2023 Annual Threat Assessment of the U.S. Intelligence Community; and CISA Joint Cybersecurity Advisory: *People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection* (AA23-144a) (dated May 24, 2023), available at https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a**.

[5] Section II.A of this SD for applicability.

System operations; and

d. Reduce the risk of exploitation of unpatched systems through the application of security patches and updates for operating systems, applications, drivers and firmware on Critical Cyber Systems in a timely manner using a risk-based methodology.

2. Develop a Cybersecurity Assessment **Plan** and submit **(a)** an annual **update, for approval,** that describes how the Owner/Operator will proactively and regularly assess the effectiveness of cybersecurity measures, and identify and resolve device, network, and/or system vulnerabilities**, and (b) an annual report that provides Cybersecurity Assessment Plan results from the previous year.** *See* Section III.F.

This revision retains the transition to a more flexible, performance-based approach requiring all Owner/Operators to submit a Cybersecurity Implementation Plan for TSA approval. All currently-identified railroad Owner/Operators have submitted a Cybersecurity Implementation Plan and are awaiting TSA approval or have a TSA-approved Cybersecurity Implementation Plan in place. This plan sets the security measures and requirements against which TSA inspects for compliance.[6] *See* Section II.B. Pursuant to 49 U.S.C. 114(f), the TSA Administrator is authorized to "enforce security-related regulations and requirements"; "inspect, maintain, and test security facilities, equipment, and systems"; and "oversee the implementation, and ensure the adequacy of security measures at … transportation facilities." Given this authority, TSA may require Owner/Operators to provide specific documentation and access to TSA as necessary to establish compliance. *See* Section IV. of this Security Directive for examples of the type of records to which TSA may require access.

Although TSA has determined that this document is not Sensitive Security Information (SSI), all information that must be reported or submitted to TSA pursuant to this Security Directive is **SSI** subject to the protections of part 1520 of title 49, Code of Federal Regulations. The Department of Homeland Security may use the information, with company-specific data redacted, for Department of Homeland Security's intelligence-derived reports. TSA and the Cybersecurity and Infrastructure Security Agency also may use information submitted for vulnerability identification, trend analysis, or to generate anonymized indicators of compromise or other cybersecurity products to prevent other cybersecurity incidents.[7] Information provided to Department of Homeland Security pursuant to this Security Directive may also be shared with other agencies as appropriate.[8]

[6] *See also* 49 U.S.C. 114(f); 49 CFR part 1503.
[7] *See* OMB Control No. 1670-0037.
[8] Presidential Policy Directive (PPD) 41 requires Federal agencies to rapidly share incident information with each other to achieve unity of governmental effort. *See* PPD-41 § III.D ("Whichever Federal agency first becomes aware of a cyber incident will rapidly notify other relevant Federal agencies in order to facilitate a unified Federal response and ensure that the right combination of agencies responds to a particular incident"). Furthermore, for purposes of information shared with the Department of Homeland Security pursuant to this directive, cyber incident responders

The distribution, disclosure, and availability of information will be restricted to persons with a need to know, and safeguarding, protecting, and marking methods for sensitive/critical information will be utilized.[9] The Office of Management and Budget (OMB) has approved this collection under OMB Control No. 1652-0074.

TSA will seek review and ratification of this Security Directive by the Transportation Security Oversight Board (TSOB). The TSOB is statutorily required to "review and ratify or disapprove" emergency regulations and security directives issued by TSA under 49 U.S.C. 114(*l*)(2). *See* 49 U.S.C. 114(*l*)(2)(B) and 115(c)(1). If the **TSOB decides not** to ratify any section or subsection of this Security Directive, or deems any section or subsection inapplicable, the remainder of this Security Directive shall not be affected **unless otherwise specified by the TSOB.**

II. ACTIONS REQUIRED

A. Applicability, Deadlines for Compliance, and Scope

1. *Applicability:* The provisions of this Security Directive apply to the following Owner/Operators:

   a. Freight Railroad Owner/Operators subject to applicability described in 49 CFR 1580.101.

   b. *Other TSA-designated Freight and Passenger Railroad Owner/Operators:* **If TSA identifies additional railroad Owner/Operators who were not already subject to the Security Directive 1580/82-2022-01 series,** TSA will notify these Owner/Operator(s) and provide specific compliance deadlines for the requirements in this Security Directive.

2. ***Managed Security Service Providers.*** **If an Owner/Operator has delegated to, or shared responsibility with, a Managed Security Service Provider, wholly or in part, for specific security measures in the Owner/Operator's Cybersecurity Implementation Plan, the Owner/Operator retains sole responsibility under this Security Directive for ensuring compliance with the Owner/Operator's TSA-approved Cybersecurity Implementation Plan and this Security Directive.**

3. ***Authorized Representative.*** **Authorized Representatives are empowered by the Owner/Operator to coordinate and/or conduct activities required by this Security Directive and/or contained within the Owner/Operator's TSA-approved Cybersecurity Implementation Plan. Both Owner/Operators and Authorized Representatives are liable for non-compliance on the part of the Authorized Representative with the applicable requirements of the**

with responsibilities under PPD-41 are "covered" persons with a "need to know," as provided by 49 CFR 1520.7 and 1520.11, respectively.

[9] *See* 49 CFR 1520.5(b)(5) and *https://www.tsa.gov/for-industry/sensitive-security-information*.

Owner/Operator's TSA-approved Cybersecurity Implementation Plan and this Security Directive.

4. *Scope:* The requirements in this Security Directive apply to Critical Cyber Systems of TSA-designated freight and passenger railroads.

   Note: If an Owner/Operator determines it has no Critical Cyber Systems, as defined in Section VII. of this Security Directive, it must notify TSA in writing within 60 days of the effective date of this Security Directive. **TSA will notify the Owner/Operator if the agency disagrees with the Owner/Operator's determination and may require the Owner/Operator to provide additional information regarding the methodologies or rationale used to identify Critical Cyber Systems. After consultation with the Owner/Operator, TSA may notify an Owner/Operator that it must include Critical Cyber Systems identified by TSA in its Cybersecurity Implementation Plan.** In the event that an Owner/Operator's method of operation changes, it must reevaluate whether it has a Critical Cyber System, and if so, **notify TSA within 60 days of the change in operations to determine the schedule for complying with the requirements of this Security Directive.**

B. Cybersecurity Implementation Plan

   1. The Cybersecurity Implementation Plan must provide all the information required by Sections III.A. through III.E. of this Security Directive and describe in detail the Owner/Operator's defense-in-depth plan, including physical and logical security controls, for meeting each of the requirements in Sections III.A. through III.E.

   2. Once approved by TSA, the Owner/Operator must implement and maintain all measures in the TSA-approved Cybersecurity Implementation Plan in accordance with the schedule as stipulated in the plan.

   3. **If an Owner/Operator needs to amend its TSA-approved Cybersecurity Implementation Plan based on revisions to this Security Directive (highlighted in bold), it must follow the procedures in Section VI.**

III. CYBERSECURITY MEASURES

The Owner/Operator must:

A. Identify the Owner/Operator's Critical Cyber Systems as defined in Section VII. of this Security Directive. **TSA will notify the Owner/Operator if the agency disagrees with the Owner/Operator's determination and may require the Owner/Operator to provide additional information regarding the methodologies or rationale used to identify Critical Cyber Systems. After consultation with Owner/Operators, TSA may notify an Owner/Operator that it must include additional Critical Cyber**

Systems identified by TSA not previously identified by the Owner/Operator in its Cybersecurity Implementation Plan.

B. Implement network segmentation policies and controls designed to prevent operational disruption to the Operational Technology system if the Information Technology system is compromised or vice-versa. As applied to Critical Cyber Systems, these policies and controls must include:

1. A list and description of —

   a. Information Technology and Operational Technology system interdependencies;

   b. All external connections to the Information Technology and Operational Technology system;

   c. Zone boundaries, including a description of how Information Technology and Operational Technology systems are defined and organized into logical zones based on criticality, consequence, and operational necessity; and

   d. Policies to ensure Information Technology and Operational Technology system services transit the other only when necessary for validated business or operational purposes.

2. An identification and description of measures for securing and defending zone boundaries, that includes security controls—

   a. To prevent unauthorized communications between zones; and

   b. To prohibit Operational Technology system services from traversing the Information Technology system, and vice-versa, unless the content is encrypted or, if not technologically feasible, otherwise secured and protected to ensure integrity and prevent corruption or compromise while the content is in transit.

C. Implement access control measures, including those for local and remote access, to secure and prevent unauthorized access to Critical Cyber Systems. These measures must incorporate the following policies, procedures, and controls:

1. Identification and authentication policies and procedures designed to prevent unauthorized access to Critical Cyber Systems that include—

a. A policy for memorized secret authenticators resets that includes criteria for when resets must occur[10]; and

b. Documented and defined mitigation measures for components of Critical Cyber Systems that will not fall under the policy required by the preceding subparagraph (III.C.1.a), and a timeframe to complete these mitigations.

2. Multi-factor authentication, or other logical and physical security controls that supplement password authentication to provide risk mitigation commensurate to multi-factor authentication. If an Owner/Operator does not apply multi-factor authentication for access to Operational Technology components or assets, the Owner/Operator must specify what compensating controls are used to manage access.

3. Policies and procedures to manage access rights based on the principles of least privilege and separation of duties. Where not technically feasible to apply these principles, the policies and procedures must describe the compensating controls that the Owner/Operator will apply.

4. Enforcement of standards that limit the availability and use of shared accounts to those that are critical for operations, and then only if absolutely necessary. When the Owner/Operator uses shared accounts for operational purposes, the policies and procedures must ensure—

a. Access to shared accounts is limited through account management that uses principles of least privilege and separation of duties; and

b. Individuals who no longer need access do not have knowledge of the password necessary to access the shared accounts.

5. Regularly updated schedule for review of existing domain trust relationships to ensure their necessity and establish policies to manage these relationships.

D. Implement continuous monitoring and detection policies and procedures that are designed to prevent, detect, and respond to cybersecurity threats and correct anomalies affecting Critical Cyber Systems. These measures must include:

1. Capabilities to—

a. Defend against malicious email, such as spam and phishing emails, to preclude or mitigate against adverse impacts to operations;

[10] This policy should be compliant with the most current version of the National Institute of Standards and Technology's Special Publication 800-63, Digital Identity Guidelines (available at https://csrc.nist.gov/publications/detail/sp/800-63/3/final).

b. Block ingress and egress communications with known or suspected malicious Internet Protocol addresses;

c. Control impact of known or suspected malicious web domains or web applications, such as by preventing users and devices from accessing malicious websites;

d. Block and prevent unauthorized code, including macro scripts, from executing; and

e. Monitor and/or block connections from known or suspected malicious command and control servers (such as Tor exit nodes, and other anonymization services).

2. Procedures to—

a. Audit unauthorized access to internet domains and addresses;

b. Document and audit any communications between the Operational Technology system and an external system that deviates from the Owner/Operator's identified baseline of communications;

c. Identify and respond to execution of unauthorized code, including macro scripts; and

d. Implement capabilities (such as Security, Orchestration, Automation, and Response) to define, prioritize, and drive standardized incident response activities.

3. Logging policies that –

a. Require continuous collection and analyzing of data for potential intrusions and anomalous behavior on Critical Cyber Systems and other Operational and Information Technology systems that directly connects with Critical Cyber Systems; and

b. Ensure data is maintained for sufficient periods, to provide effective investigation of cybersecurity incidents.

4. Mitigation measures or manual controls to ensure industrial control systems can be isolated when a cybersecurity incident in the Information Technology system creates risk to the safety and reliability of the Operational Technology system.[11]

E. Reduce the risk of exploitation of unpatched systems through the application of security patches and updates for operating systems, applications, drivers, and firmware on Critical

[11] *See* related requirement in Section **D**.1.a. in the SD 1580-21-01 series.

Cyber Systems consistent with the Owner/Operator's risk based methodology. These measures must include:

1. A patch management strategy that ensures all critical security patches and updates on Critical Cyber Systems are current.

2. The strategy required by Section III.E.1. must include:

    a. The risk methodology for categorizing and determining criticality of patches and updates, and an implementation timeline based on categorization and criticality; and

    b. Prioritization of all security patches and updates on the Cybersecurity and Infrastructure Security Agency's Known Exploited Vulnerabilities Catalog.[12]

3. If the Owner/Operator cannot apply patches and updates on specific Operational Technology systems without causing a severe degradation of operational capability to meet necessary capacity, the patch management strategy must include a description and timeline of additional mitigations that address the risk created by not installing the patch or update.

F. Develop a Cybersecurity Assessment **Plan** for proactively assessing and auditing cybersecurity measures.

1. The Owner/Operator must develop a Cybersecurity Assessment **Plan** for proactively assessing Critical Cyber Systems to ascertain the effectiveness of cybersecurity measures and to identify and resolve device, network, and/or system vulnerabilities.

2. The Cybersecurity Assessment **Plan** required by Section III.F.1. must –

    a. Assess the effectiveness of the Owner/Operator's TSA-approved Cybersecurity Implementation Plan;

    b. Include a **cybersecurity** architecture design review to be conducted within the first 12 months after the Cybersecurity Implementation Plan approval and at least once every two years thereafter. A **cybersecurity** architecture design review contains verification and validation of network traffic, a system log review, and analysis to identify cybersecurity vulnerabilities related to network design, configuration, and inter-connectivity to internal and external systems; and

    c. Incorporate other assessment capabilities designed to identify vulnerabilities based on evolving threat information and adversarial capabilities, such as

[12] Available at: https://www.cisa.gov/known-exploited-vulnerabilities-catalog.

penetration testing of Information Technology systems, including the use of "red" and "purple" team (adversarial perspective) testing.

d. **Include a schedule for assessing and auditing specific cybersecurity measures and/or actions required by subparagraphs F.2.a. through F.2.c. of this section. The schedule must ensure that at least one-third (1/3) of the policies, procedures, measures, and capabilities in the TSA-approved Cybersecurity Implementation Plan are assessed each year, with 100 percent assessed over any three-year period; and**

e. **Ensure an annual report of the results of assessments conducted in accordance with the Cybersecurity Assessment Plan is submitted to TSA as described in paragraph F.4. of this section. The required report must indicate—**

i. For the previous 12 months, which assessment method(s) were used to determine whether the policies, procedures, and capabilities described by the Owner/Operator in its Cybersecurity Implementation Plan are effective; and

ii. Results of the individual assessments conducted in the previous 12 months.

3. **The Owner/Operator must review and update its Cybersecurity Assessment Plan on an annual basis and submit it to TSA for approval no later than 12 months from the date the Owner/Operator *submitted* its first Cybersecurity Assessment Plan under Security Directive 1580/82-2022-01. The next Cybersecurity Assessment Plan submitted under this Security Directive, and all other Cybersecurity Assessment Plans thereafter, must be submitted to TSA no later than 12 months from the date of TSA's *approval* of the most recent Cybersecurity Assessment Plan.**

4. **The Owner/Operator must submit the Cybersecurity Assessment Plan report required by subparagraph F.2.e. of this section on an annual basis but no later than 12 months from the date the Owner/Operator *submitted* its first Cybersecurity Assessment Plan under Security Directive 1580/82-2022-01. The next Cybersecurity Assessment Plan report submitted under this Security Directive, and all other Cybersecurity Assessment Plan reports thereafter, must be submitted to TSA no later than 12 months from the date of TSA's *approval* of the most recent Cybersecurity Assessment Plan.**

IV. RECORDS

A. *Use of previous plans, assessments, tests, and evaluations.* As applicable, Owner/Operators may use previously developed plans, assessments, tests, and evaluations to meet the requirements of this Security Directive. If the Owner/Operator

relies on these materials, it must include an index of the records and their location organized in the same sequence as the requirements in this Security Directive. **In addition, these materials must be explicitly incorporated by reference into the Cybersecurity Implementation Plan and made available to TSA upon request.**

B. *Protection of sensitive security information.* The Owner/Operator must, at a minimum, store and transmit the following information required by this Security Directive consistent with the requirements in 49 CFR part 1520:[13]

1. Plans and reports; and

2. Audit, testing, or assessment results.

C. *Documentation to Establish Compliance*

1. The Owner/Operator must make records necessary to establish compliance with this Security Directive available to TSA upon request for inspection and/or copying.

2. TSA may request to inspect or copy the following documents to establish compliance with this Security Directive:

   a. Hardware/software asset inventory, including supervisory control, and data acquisition systems.

   b. Firewall rules.

   c. Network diagrams, switch and router configurations, architecture diagrams, publicly routable internet protocol addresses, and Virtual Local Area Networks.

   d. Policy, procedural, and other documents that informed the development, and documented implementation of, the Owner/Operator's Cybersecurity Implementation Plan, Cybersecurity Incident Response Plan, Cybersecurity Assessment Program, and assessment or audit results.

   e. Data providing a "snapshot" of activity on and between Information and Operational Technology systems such as –

      i. Log files;

      ii. A capture of network traffic (e.g., packet capture (PCAP)), not to exceed a period of twenty-four hours, as identified and directed by TSA;

[13] Owner/Operators may contact SSI@tsa.dhs.gov for more information on how to comply with requirements for the protection of Sensitive Security Information.

iii. "East-West Traffic" of Operational Technology systems/sites/environments within the scope of this Security Directive's requirements; and

iv. "North-South Traffic" between Information and Operational Technology systems, and the perimeter boundaries between them.

f. Any other records or documents necessary to establish compliance with this Security Directive.

V. PROCEDURES FOR SECURITY DIRECTIVES

A. General Procedures

1. *Confirm Receipt.* Immediately provide written confirmation of receipt of this Security Directive via e-mail to SurfOpsRail-SD@tsa.dhs.gov;

2. *Dissemination.* Immediately disseminate the information and measures in this Security Directive to corporate senior management and security management representatives. The Owner/Operator must provide the applicable security measures in this Security Directive to the Owner/Operator's direct employees and authorized representatives responsible for implementing applicable security measures as necessary to ensure compliance.

B. *Comments.* Owner/Operators may comment on this Security Directive by submitting data, views, or arguments in writing to TSA via e-mail at TSA-Surface@tsa.dhs.gov. Any comments referring to specific measures in this Security Directive must be protected in accordance with the requirements in 49 CFR part 1520. TSA may amend the Security Directive based on comments received. Submission of a comment does not delay the effective date of the Security Directive or requirement to comply with the provisions of the Security Directive.

C. ***Submission of Documentation to TSA:*** **Owner/Operators are required to submit documents in a manner prescribed by TSA. TSA will provide Owner/Operators specific instructions for submission of required documents.**

VI. AMENDMENTS TO CYBERSECURITY IMPLEMENTATION PLAN

A. *Changes to ownership or control of operations.* An Owner/Operator required to submit a Cybersecurity Implementation Plan under Section II.B. of this Security Directive must submit a request to amend its Cybersecurity Implementation Plan if, after approval, there are any changes to the ownership or control of the operation.

B. *Changes to conditions affecting security*. An Owner/Operator required to submit a Cybersecurity Implementation Plan under Section II.B. of this Security Directive must submit a request to amend its Cybersecurity Implementation Plan if, after approval, the Owner/Operator makes, or intends to make, permanent changes to the policies,

procedures, or measures approved by TSA, including, but not limited to changes to address:

1. Determinations that a specific policy, procedure, or measure in the Cybersecurity Implementation Plan is ineffective based on results of the audits and assessments required under Section III.F. of this Security Directive; or

2. The Owner/Operator has identified or acquired new or additional Critical Cyber Systems or capabilities for meeting the requirements in the Security Directive that have not been previously approved by TSA.

C. *Permanent change*. For purposes of this section, a "permanent change" is one intended to be in effect for 45 or more days.

D. *Schedule for requesting amendment*. The Owner/Operator must file the request for an amendment to its Cybersecurity Implementation Plan with TSA no later than 50 days after the permanent change takes effect, unless TSA allows a longer time period.

E. *TSA approval*.

1. TSA may approve a requested amendment to a Cybersecurity Implementation Plan if TSA determines that it is in the interest of public and transportation security and the proposed amendment provides the level of security required under this Security Directive.

2. TSA may request additional information from the Owner/Operator before rendering a decision.

F. *Petition for reconsideration*. No later than 30 days after receiving a denial of an amendment to a Cybersecurity Implementation Plan, the Owner/Operator may file a petition for reconsideration following the procedures set in 49 CFR 1570.119.

VII. DEFINITIONS

In addition to the terms defined in 49 CFR 1500.3, 1570.3 and the Security Directive 1580-21-01 **series** and Security Directive 1582-21-01 **series**, the following terms apply to this Security Directive:

A. ***Authorized Representative*** **means, for the purpose of this Security Directive, a person who is not a direct employee of the Owner/Operator, but is authorized to act on the Owner/Operator's behalf to perform measures required by the Security Directive and/or contained within the Owner/Operator's TSA-approved Cybersecurity Implementation Plan. The term authorized representative may include agents, contractors, and subcontractors. This term does not include Managed Security Service Providers.**

B. *Critical Cyber System* means any Information or Operational Technology system or data that, if compromised or exploited, could result in operational disruption. Critical Cyber Systems include those business services that, if compromised or exploited, could result in operational disruption.

C. *Cybersecurity Architecture Design Review* means a technical assessment based on government and industry-recognized standards, guidelines, and best practices that evaluates systems, networks, and security services to determine if they are designed, built, and operated in a reliable and resilient manner. These reviews must be designed to be applicable to the Owner/Operator's Information and Operational Technology systems.

D. *Cybersecurity incident* means an event that, without lawful authority, jeopardizes, disrupts or otherwise impacts, or is reasonably likely to jeopardize, disrupt or otherwise impact, the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident on the system. This definition includes an event that is under investigation or evaluation by the Owner/Operator as a possible cybersecurity incident without final determination of the event's root cause or nature (such as malicious, suspicious, **or** benign).

E. *Days* means calendar days unless otherwise indicated. As used for compliance deadlines, if a requirement must be met on a date that is a national holiday, the compliance deadline will be the next federal business day after the holiday.

F. *East-West traffic* means, in a networking context, the lateral movement of network traffic within a trust zone or local area network.

G. *Group policy* means a centralized place for administrators to manage and configure operating systems, applications and users' settings that can be used to increase the security of users' computers and help defend against both insider threats and external attacks.

H. *Information Technology system* means any services, equipment, or interconnected systems or subsystems of equipment that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information that fall within the responsibility of the Owner/Operator to operate and maintain.

I. *Interdependencies* means relationships of reliance within and among Information and Operational Technology systems that must be maintained for those systems to operate and provide services.

J. ***Managed Security Service Providers*** **means for the purposes of this Security Directive, a person who is not a direct employee of the Owner/Operator, but who provides one or more services or capabilities that the Owner/Operator is using to**

perform measures required by the Security Directive and/or contained within the Owner/Operator's TSA-approved Cybersecurity Implementation Plan. Managed Security Service Providers generally provide a logical service or capability. Managed Security Service Providers are not Authorized Representatives.

K. *Memorized secret authenticator* means a type of authenticator comprised of a character string intended to be memorized by, or memorable to, the subscriber, permitting the subscriber to demonstrate something they know as part of an authentication process

L. *Necessary capacity* means the Owner/Operator's determination of capacity to support its business critical functions required for railroad operations and supply chain expectations.

M. *North-South traffic* means network traffic that moves through a perimeter boundary into another trust level.

N. *Operational disruption,* for purposes of this Security Directive, means a deviation from or interruption of necessary capacity that results from a compromise or loss of data, system availability, system reliability, or control of a railroad subject to this Security Directive.

O. *Operational Technology system* is a general term that encompasses several types of control systems, including industrial control systems, supervisory control and data acquisition systems, distributed control systems, and other control system configurations, such as programmable logic controllers, fire control systems, and physical access control systems, often found in the industrial sector and critical infrastructure. Such systems consist of combinations of programmable electrical, mechanical, hydraulic, pneumatic devices or systems that interact with the physical environment or manage devices that interact with the physical environment.

P. *Owner/Operator* means a railroad carrier that operates rolling equipment on track that is part of the general railroad system of transportation.

Q. *Phishing* means tricking individuals into disclosing sensitive personal information through deceptive computer-based means such as internet web sites or e-mails using social engineering or counterfeit identifying information.

R. *Security, Orchestration, Automation, and Response (SOAR)* means capabilities that enable Owner/Operators to collect inputs monitored by the security operations team. For example, alerts from the security information and event management system and other security technologies – where incident analysis and triage can be performed by leveraging a combination of human and machine power – help define, prioritize and drive standardized incident response activities. These capabilities allow an Owner/Operator to define incident analysis and response procedures in a digital workflow format.

S. *Shared account* means an account that is used by multiple users with a common authenticator to access systems or data. A shared account is distinct from a group

account, which is a collection of user accounts that allows administrators to group similar user accounts together in order to grant them the same rights and permissions. Group accounts do not have common authenticators.

T. *Spam* means electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

U. *Tor*, also known as The Onion Router, means software that allows users to browse the web anonymously by encrypting and routing requests through multiple relay layers or nodes. Tor software obfuscates a user's identity from anyone seeking to monitor online activity (such as nation states, surveillance organizations, information security tools). This deception is possible because the online activity of someone using Tor software appears to originate from the Internet Protocol address of a Tor exit node, as opposed to the address of the user's computer.

V. *Trust relationship* means an agreed upon relationship between two or more system elements that is governed by criteria for secure interaction, behavior, and outcomes relative to the protection of assets. This term refers to trust relationships between system elements implemented by hardware, firmware, and software.

W. *Unauthorized access of an Information Technology or Operational Technology system* means access from an unknown source; access by a third party or former employee; an employee accessing systems for which he or she is not authorized; and may include a non-malicious Owner/Operator policy violation such as the use of a shared credential by an employee otherwise authorized to access it.

STACEY D FITZMAURICE

Digitally signed by STACEY D FITZMAURICE
Date: 2023.10.20 15:49:43 -04'00'

Stacey Fitzmaurice
Executive Assistant Administrator
Operations Support